REMARKS

Claims 1-9, 11-14 and 36-42 are pending in the present application. In the above amendments, claims 1, 2, 5, 9, 11, 14 and 38-40 have been amended, and claims 41-42 have been added, and claims 3-4, 10, 15-16, 18-29, 31-32 and 34 have been canceled.

Applicants respectfully respond to this Office Action.

Claim Rejections – 35 USC § 103(a)

Claims 1-9, 11-14 and 36-40 have been rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,243,468 to Pearce et al., in view of U.S. Patent No. 6,931,545 to Ta et al., and further in view of Gralla, in How the Internet Works.

The rejection of claim 1 as allegedly unpatentable over the Pearce patent in view of the Ta patent, and further in view of the Gralla publication, is respectfully traversed. Claim 1, as amended, recites "a method of validating an association of software code with hardware, comprising: obtaining a certificate from a code image, wherein: the code image further including software code, a code signature, and a first identifier associated with a release of the software code, all instances of the software code associated with the software release have the same first identifier such that at least two instances of the software code have the same first identifier, the code signature is generated, using cryptography and a code private key, based on the first identifier, a second identifier for the hardware, and a message code digest obtained by hashing the software code, the code signature is used to validate an association of the software code with the hardware, the certificate includes a code public key corresponding to the code private key, and an authority signature generated over the code public key using cryptography and an authority private key; authenticating the certificate with an authority public key securely stored in the hardware; obtaining the first identifier from the code image; obtaining the second identifier for the hardware, wherein all instances of a particular configuration of the hardware have the same second identifier such that at least two instances of the hardware have the same second identifier; obtaining the software code from the code image and generating an image code digest by hashing the software code from the code image; generating a regenerated signature digest by hashing the image code digest, the first identifier, and the second identifier; obtaining

the code signature from the code image and generating a received signature digest by decrypting the code signature from the code image using the code public key; and comparing the regenerated signature digest with the received signature digest, wherein the association of the software code with the hardware is validated if the regenerated signature digest matches the received signature digest."

Applicants assert that the Pearce patent, the Ta patent, and the Gralla publication fail to disclose a code image including the software code, a code signature, a first identifier associated with a release of the software code, and a certificate including a code public key corresponding to a code private key and an authority signature generated over the code public key using cryptography and an authority private key. The Pearce patent and the Ta patent do not disclosure code public and private keys, or an authority private key. The Gralla publication discloses using digital signatures to verify the origin of a message, using a random key to encrypt the message, and forwarding the random key encrypted by the receiver's public key to the receiver. However, the Gralla publication fails to disclose an authority signature generated over the code public key using cryptography and an authority private key.

Further , the Pearce patent, the Ta patent, and the Gralla publication fail to disclose that the code signature is generated, using cryptography and a code private key, based on the first identifier, a second identifier for the hardware, and a message code digest obtained by hashing the software code. The Pearce patent discloses computing a "test ID from the product ID and hardware ID using the same algorithm (e.g., hashing algorithm) . . ." (column 3, lines 1-10), without mention of a code signature also based on the message code digest obtained by hashing the software code. The Ta patent and the Gralla publication fail to remedy this disclosure deficiency of the Pearce patent.

Further, claim 1 recites that the authority public key is securely stored in the hardware. The Gralla Publication discloses that the "public key is made freely available, whereas the private key is kept secret on the person's computer." See, page 303. Thus, the Gralla Publication teaches away from securely storing the authority public key in the hardware. Therefore, Applicants assert that one skilled of the art would not be motivated to securely store an authority public key in hardware for the purpose of validating an association of software code with the hardware, absent the teachings of the applicants' disclosure.

Accordingly, the rejection of claim 1 as allegedly unpatentable over the Pearce patent in view of the Ta patent, and further in view of the Gralla publication, should be withdrawn.

The amendments to claim 1 are supported by Figures 2-5 and 9-10, and by the corresponding descriptions in the specification.

It is respectfully submitted that dependent claims 2-8 are at least allowable for the reasons given above in relation to independent claim 1.

Claims 9 and 14 are apparatus claims defined by language similar to that of claim 1. For reasons similar to those discussed above with respect to claim 1, the rejections of claims 9 and 14, as allegedly unpatentable over the Pearce patent in view of the Ta patent, and further in view of the Gralla publication, should be withdrawn.

It is respectfully submitted that dependent claims 11-13 and 38-40 are at least allowable for the reasons given above in relation to independent claims 1, 9 and 14.

Further, regarding claims 38-40, these claims recite that "the authority public key is embedded in the hardware in a tamper-proof manner." The respective independent claims recite that the "authority public key" is "securely stored in the hardware". In the Office Action, the Examiner took "official notice that it well known in the art to store secure information in a tamper-proof manner." Applicants traverse the Examiner's factual finding as support for the proposition that securely storing an authority public key by embedding it in the hardware in a tamper-proof manner is well known in the art. Generally, a public key is made public. As disclosed in the Gralla Publication, the "public key is made freely available, whereas the private key is kept secret on the person's computer." See, page 303. Thus, it is well known in the art to leave a public key unsecure and freely available. Further, "assertions of technical facts in areas of esoteric technology . . . must always be supported by citation to some reference work recognized as standard in the pertinent art." See, MPEP, 2144.03 (A). In accordance with MPEP 2144.03 (C), Applicants request that the Examiner produce documentary evidence or authority to support his statement taking official notice of well known art.

The rejection of claim 36 as allegedly unpatentable over the Pearce patent in view of the Ta patent, and further in view of the Gralla publication, is respectfully traversed. Claim 36 recites "an apparatus operable to validate software for hardware, comprising: a storage device configured to store a code image including the software, a code signature, and a certificate; [and]

a secure storage device configured to store a hardware identifier and a certificate authority public key." Further, claim 36 recites decrypting "the certificate using the certificate authority public key to recover a code public key". The Gralla Publication discloses that the "public key is made freely available, whereas the private key is kept secret on the person's computer." See, page 303. Thus, the Gralla Publication teaches away from a secure device configured to store a certificate authority public key, and a processor configured to decrypt the certificate using the certificate authority public key to recover a code public key. Accordingly, Applicants assert that claim 36 defines a patent advance over the Pearce patent in view of the Ta patent, and further in view of the Gralla publication, and that the rejection of claim 36 should be withdrawn.

It is respectfully submitted that dependent claim 37 is at least allowable for the reasons given above in relation to independent claim 36, and dependent claims 38-40.
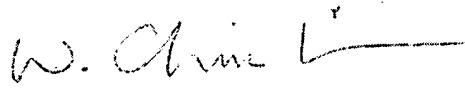
New Claims

New claim 41 is supported by Figures 2-5 and 9-10, and by the corresponding descriptions in the specification. New claim 42 is supported by the descriptions at page 5, paragraph [1028], and page 11, paragraph [1054]. Applicants respectfully assert that new claims 41-42 recite patentable features over the cited prior art and should be allowed.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **December 4, 2008**

By: **Won Tae C. Kim, Reg. # 40,457**
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502